TRANSMITTAL LETTER (General - Patent Pending)	Docket No. 86503-50

In Re Application Of: **Tet Hin YEAP et al.**

Application No.	Filing Date	Examiner	Customer No.	Group Art Unit	Confirmation No.
10/673,509	September 30, 2003	Shawki Saif ISMAIL	28291	2155	1659

Title: **SYSTEM AND METHOD FOR SECURE ACCESS**

COMMISSIONER FOR PATENTS:

Transmitted herewith is:

- AMENDED SUMMARY OF CLAIMED SUBJECT MATTER IN RESPONSE TO THE NOTIFICATION OF NON-COMPLIANT APPEAL BRIEF OF OCTOBER 6, 2008.

in the above identified application.

- ☒ No additional fee is required.
- ☐ A check in the amount of is attached.
- ☒ The Director is hereby authorized to charge and credit Deposit Account No. **19-2550** as described below.
  - ☐ Charge the amount of
  - ☐ Credit any overpayment.
  - ☒ Charge any additional fee required.
- ☐ Payment by credit card. Form PTO-2038 is attached.

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

Signature

Dated: **November 3, 2008**

Sanro Zlobec, Reg. No. 52,535
SMART & BIGGAR
1000 De La Gauchetière Street West
Suite 3300
Montreal, Quebec H3B 4W5
CANADA

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to the "Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450" [37 CFR 1.8(a)] on

_____.
(Date)

Signature of Person Mailing Correspondence

Typed or Printed Name of Person Mailing Correspondence

cc:

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Re:	U.S. Patent Application of Tet Hin YEAP *et al.*		
App. No.:	10/673,509	Group Art Unit:	2155
Filed:	September 30, 2003	Examiner:	Shawki Saif ISMAIL
For:	SYSTEM AND METHOD FOR SECURE ACCESS		

AMENDED SUMMARY OF CLAIMED SUBJECT MATTER IN RESPONSE TO THE NOTIFICATION OF NON-COMPLIANT APPEAL BRIEF OF OCTOBER 6, 2008

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

In response to the Notification of Non-Compliant Appeal Brief mailed October 6, 2008, submitted herewith is an Amended Summary of Claimed Subject Matter in accordance with 37 CFR §41.37. As set forth in MPEP §1205.03, an entire new Appeal Brief is not being filed herewith but rather a summary of the claimed subject matter as required.

It is believed that no fees are due. However, if any fees are due, the Director is hereby authorized to debit the required amount from deposit account no. 19-2550 and to advise the Applicant accordingly.

I. Remarks

In the Notification of Non-Compliant Appeal Brief, the Examiner alleges that the Appeal Brief submitted by the Applicant on July 10, 2008 "merely identifies limitations rather than elements of the claim". In response, the Applicant has broken down the claims into charts with specific relevant cross-references for individual items referred to in the claims. The Applicant has also maintained references to certain passages relevant to the overall understanding of the claims.

II. 37 CFR §41.37 (c)(1)(v) - Amended Summary of Claimed Subject Matter

The present application includes forty-six (46) claims, of which independent claims 35, 45, 56, 67, 68, 70, 72, 74 are being appealed. Independent claim 70 is the only claim being appealed comprising "means plus function" limitations as under 35 USC §112, sixth paragraph. A summary of independent claims 35, 45, 56, 67, 68, 70, 72, 74 is provided below. References herein refer to the specification and drawings as originally filed.

Brief Overview:

In order to assist the Board of Patent Appeals and Interferences in understanding the claims at issue in this Appeal, the Applicant presents herewith a brief overview of the invention, which overview is not intended to limit or define the invention but is merely intended to serve as context. The invention is defined, rather, by the language of the claims. The claims are paraphrased further below and sub-divided into tabular entries to allow cross-referencing to particular specification page and line numbers and reference numerals in the figures.

The claims are directed to methods, apparatus and systems for authentication in the context of providing secure remote access to computer equipment. When it is desired to obtain remote access to a certain computer equipment such as a telecommunication switch (Figure 1, 50) in a remote office from a remote client (Figure 1, 42), it is critical that the access be secure. An authentication server (Figure 1, 38) may be used as a trusted third party to assist in providing security in communications between the client and the office (page 5, lines 15-17). The authentication server can have and deliver complement-pair keys for use in encrypted communications, one to the client and one to the office (Figure 2, 240; Figure 3, 355; page 9, lines 19-21; page 15, lines 1-7). The key being sent to the client may only be sent under the condition that the client authenticates the user's identity with the server; the authentication communication can be wholly or partly encrypted (Figure 3, 310-355; page 14, line 1 – page 15, line 8).

The remote office may also comprise an access controller (Figure 1, 54) that controls access to the computer equipment. For example, the access controller may authenticate that communications between the client and the computer equipment are authorized and may selectively permit such communications to be passed (page 6, lines 1-4).

Summary of Independent Claims being Appealed:

The specific language of each independent claim at issue in this appeal is paraphrased below in the following charts which set forth items described in the specification, including the figures, that are read upon by the claims, making specific reference to specification page and line numbers and reference numerals in the figures. However, it should be understood that any association between claim language and teachings of the specification are not limiting but instead merely identify corresponding components of illustrative embodiments described in the specification.

Claim 35

Claim 35 is a system claim directed to an authentication system.

Elements of the claim	Items read upon by the element
Claim 35 is directed to an authentication system.	(Fig 1, 30; page 4, lines 17-22)
The authentication system comprises an access controller	(Fig 1, 54; page 5, lines 1-11)
that is operable to communicate with a client	(Fig 1, 42; page 5, lines 21-28)
via a first communication medium.	(page 5, lines 1-11; page 19, line 1 – page 20, line 3)
The authentication system further comprises an authentication server	(Fig 1, 38; page 5, lines 12-17)
that is operable to communicate with the client and the access controller via a second communication medium.	(page 5, lines 12-20; page 19, line 1 – page 20, line 3)
The authentication server is further operable to deliver a first key to the client	(Fig. 3, 355; page 5, lines 17-26; page 15, lines 1-8)
and a second key to the access controller.	(Fig 2, 240; page 5, lines 17-26; page 9, lines 19-21)
The second key is complementary to the first key	(page 5, lines 15-19)
such that when the client and the access controller are connected, communications therebetween can be encrypted using the keys.	(page 5, lines 13-20, page 5, lines 21-28; Fig 4, 420-430; page 16, lines 12-21; page 18, lines 7-16)
The access controller is further operable to selectively pass instructions received from the client to a computer attached to the access controller if a verification protocol utilizing the keys is met	(Fig 4, 435-440; page 16, line 22 – page 17, line 3).
The first key is delivered to the client only if a user operating the client authenticates the user's identity with the server.	(Fig 3, 310-355; page 14, line 1 – page 15, line 8).

Claim 45

Claim 45 is an apparatus claim directed to an access controller.

Elements of the claim	Items read upon by the element
Claim 45 is directed to an access controller	(Fig 1, 54; page 5, lines 5-9; page 6,

	lines 1-7)
for intermediating communications between	(page 6, lines 1-7)
an interface	(Fig 1, 58; page 5, lines 6-9)
and a computer	(Fig. 1, 34, 50; page 5, lines 1-11; page 19, lines 1-4; page 20, lines 4-9)
and operable to store a second key complementary to a first key.	(Table 1; Fig 1, 62; page 5, lines 15-26; page 6, line 12 – page7, line 17; page 9, lines 19-21; Table III; page 11, lines 1-3; page 15, lines 1-8)
The access controller is further operable to communicate with a client via the interface.	(Fig 1, 58; page 5, lines 1-11)
The client is operable to store the first key	(Table V; Fig 1, 70; page 5, lines 21-28; page 12, line 18 – page 13, line 2; Table VII)
and to receive instructions from a user.	(page 16, lines 8-11)
The access controller is still further operable to selectively pass the instructions to the computer if a verification protocol utilizing the keys is met.	(Fig 4, 435-440; page 16, line 22 – page 17, line 3)
The verification protocol includes the generation of a random number by the client and an encryption of the random number by the client using the first key.	(Fig. 4, 415-420; page 16, lines 12-18)
The random number and the encrypted random number are delivered from the client to the access controller.	(Fig. 4, 425; page 16, lines 12-18)
The encrypted random number is decrypted using the second key by the access controller	(Fig. 4, 430; page 16, lines 19-21)
and a comparison of the random number and the decrypted number is made.	(Fig. 4, 435; page 16, lines 22-27)
If the comparison finds a match of the random number with the decrypted random number, the decision is made to pass at least a portion of the instructions.	(Fig. 4, 435-440; page 16, line 22 – page 17, line 3)
If no match is found, a decision is made not to pass the at least a portion of the instructions.	(Fig. 4, 435; page 16, lines 22-27)

Claim 56

Claim 56 is a method claim directed to a method in an authentication server.

Elements of the claim	Items read upon by the element
Claim 56 is directed to a method,	(Fig. 2, 200; page 8, line 14 – page11, line 15)
in an authentication server,	(Fig 1, 28; page 5, lines 12-17)
of securing access between a client	(Fig 1, 42; page 5, lines 21-28)
having temporary connection to a computer	(Fig 1, 50; page 5, lines 1-11; page 19, lines 1-4; page 20, lines 4-9)
via an access controller.	(Fig 1, 54; page 5, lines 1-11)
The access controller is for selectively passing instructions received from the client to the computer if a verification protocol utilizing a set of keys is met.	(page 6, lines 1-7; Fig. 4, 435-440; page 16, lines 8-11; page 16, line 22 – page 17, line 3)
The method comprises receiving a request from the access controller	(Fig. 2, 220; page 9, lines 6-14)
for an updated first key.	(Fig. 2, 230; page 9, lines 15-18)
The request is authenticated.	(Fig. 2, 220; page 9, lines 6-14)
The updated first key and a second key corresponding to the updated first key are determined.	(Fig. 2, 230; page 9, lines 15-18)
The updated first key is delivered to the access controller.	(Fig. 2, 240; page 9, lines 19-21)

Claim 67

Claim 67 is a method claim directed to a method involving a client and a computer having an access controller.

Elements of the claim	Items read upon by the element
Claim 67 is directed to a method	(Fig. 4, 400; page 15, line 17 – page 17, line 5)
of securing access between a client	(Fig. 1, 42; page 5, lines 21-28)
and a computer	(Fig. 1, 34, 50; page 5, lines 1-11; page 19, lines 1-4; page 20, lines 4-9)
having an access controller	(Fig 1, 54; page 5, lines 1-11)
intermediate the client and the computer. The client	(Fig. 4, 410; page 16, lines 8-11)

receives an instruction destined for the computer	
and generates a random number.	(Fig. 4, 415, page 16, lines 12-18)
The client encrypts the random number using a first key.	(Fig.4, 420; page 5, lines 17-26; page 16, lines 12-18)
The random number, the encrypted random number and the instruction are delivered to the access controller.	(Fig. 4, 425; page 16, lines 12-18)
The access controller decrypts the encrypted random number using a second key, the second key being complementary to the first key.	(Fig. 4, 430; page 5, lines 17-26; page 16, lines 19-21)
The random number and the decrypted number are compared.	(Fig. 4, 435; page 16, lines 22-27)
If the comparison finds a match of the random number with the decrypted number, at least a portion of the instruction is passed to the computer.	(Fig. 4, 440; page 16, line 22 – page 17, line 3)
If no match is found, the at least a portion is discarded.	(Fig. 4, path "Discard Instruction"; page 16, lines 22-27)

Claim 68

Claim 68 is an apparatus claim directed to an authentication server.

Elements of the claim	Items read upon by the element
Claim 68 is directed to an authentication server	(Fig 1, 38; page 5, lines 12-17)
comprising an interface	(page 5, lines 13-20)
for communicating with a client	(Fig. 1, 42; page 5, lines 21-28)
and an access controller	(Fig. 1, 54; page 5, lines 1-11)
via a communication medium	(Fig 1, 46; page 5, lines 1-11; page 19, line 1- page 20, line 3)
and a processing unit.	(page 5, lines 13-20)
The processing unit is operable to determine a first key for delivery to the client and a second key for delivery to the access controller.	(page 5, lines 13-26; page 9, lines 15-18)
The first key is delivered to the client only if a user operating the client authenticates the user's identity with the server.	(Fig 3, 310-355; page 14, line 1 – page 15, line 8)

When the access controller and the client are connected, the access controller selectively passes instructions from the access controller if a verification protocol utilizing the keys is met.	(page 6, lines 1-7; Fig. 4, 435-440; page 16, line 22 – page 17, line 3)

Claim 70

Claim 70 is an apparatus claim directed to an authentication server that comprises means plus function. Means plus function are identified with asterisks (*).

Elements of the claim	Items read upon by the element
Claim 70 is directed to an authentication server	(Fig 1, 38; page 5, lines 12-17)
for securing access between a client	(Fig. 1, 42; page 5, lines 21-28)
having temporary connection and a computer	(Fig. 1, 34, 50; page 5, lines 1-11; page 19, lines 1-4; page 20, lines 4-9)
via an access controller.	(Fig 1, 54; page 5, lines 1-11)
The access controller is for selectively passing instructions received from the client to the computer if a verification protocol utilizing a set of keys is met.	(page 6, lines 1-7; Fig. 4, 435-440; page 16, lines 8-11; page 16, line 22 – page 17, line 3)
*The authentication server comprises means for receiving a request from the access controller for an updated first key,	(page 5, lines 1-20 Fig. 2, 220; page 9, lines 6-14)
*means for authenticating the request,	(page 5, lines 1-20; Fig. 2, 220; page 9, lines 6-14)
*means for determining the updated first key and a second key corresponding to the updated first key,	(page 5, lines 1-20; Fig. 2, 230; page 9, lines 15-18)
*and means for delivering the updated first key to the access controller.	(page 5, lines 1-20; Fig. 2, 240; page 9, lines 19-21)

Claim 72

Claim 72 is a method claim directed to a method in an access controller.

Elements of the claim	Items read upon by the element
Claim 72 is directed to a method,	(Fig. 5, 500; page 17, line 6 – page 18,

	line 6)
in an access controller	(Fig 1, 54; page 5, lines 1-11)
for selectively passing instructions between a client	(Fig. 1, 42; page 5, lines 21-28)
and a computer	(Fig. 1, 34, 50; page 5, lines 1-11; page 19, lines 1-4; page 20, lines 4-9)
if a verification protocol is met,	(page 6, lines 1-7; Fig. 4, 435-440; page 16, line 22 – page 17, line 3)
of expiring the verification protocol. The method comprises determining if a first preset period of time since the client disconnected from the access controller has elapsed.	(Fig. 5, 510; page 17, lines 6-20)
The method also comprises determining if a second preset period of time since the verification protocol was updated has elapsed.	(Fig. 5, 520; page 17, line 21 – page 21, line 2)
The verification protocol is expired by refusing to pass the instructions if either of the preset periods of time have elapsed.	(Fig. 5, 515; page 17, line 6 – page 18, line 2)

Claim 74

Claim 74 is an apparatus claim directed to an authentication system.

Elements of the claim	Items read upon by the element
Claim 74 is directed to an authentication system.	(Fig 1, 30; page 4, lines 17-22)
The authentication system comprises an access controller	(Fig 1, 54; page 5, lines 1-11)
that is operable to communicate with a client	(Fig 1, 42; page 5, lines 21-28)
via a first communication medium.	(page 5, lines 1-11; page 19, line 1 – page 20, line 3)
The authentication system further comprises an authentication server	(Fig 1, 38; page 5, lines 12-17)
that is operable to communicate with the client and the access controller via a second communication medium.	(page 5, lines 12-20; page 19, line 1 – page 20, line 3)
The authentication server is further operable to deliver a first key to the client	(Fig. 3, 355; page 5, lines 17-26; page 15, lines 1-8)

and a second key to the access controller.	(Fig 2, 240; page 5, lines 17-26; page 9, lines 19-21)
The second key is complementary to the first key	(page 5, lines 15-19)
such that when the client and the access controller are connected, communications therebetween can be encrypted using the keys.	(page 5, lines 13-20, page 5, lines 21-28; Fig 4, 420-430; page 16, lines 12-21; page 18, lines 7-16)
The access controller is further operable to selectively pass instructions received from the client	(Fig 4, 435-440; page 16, lines 8-11; page 16, line 22 – page 17, line 3)
to a computer attached to the access controller if a verification protocol utilizing the keys is met.	(Fig. 1, 34, 50; page 5, lines 1-11; page 19, lines 1-4; page 20, lines 4-9)
The access controller contains a preset second key	(Table I; Fig 1, 62; page 6, line 1 – page 7, line 17)
and the authentication server maintains a record of the preset second key.	(Table II; Fig. 1, 66; page 7, line 25 – page 8, line 13)
The authentication server is operable to deliver the first key and the second key only if the access controller successfully transmits the preset second key to the authentication server and the transmitted preset second key matches the authentication server's record thereof.	(Fig. 2, 200; page 8, line 14 – page11, line 15)

CONCLUSION

It is respectfully submitted that the Amended Summary of Claimed Subject Matter submitted herewith satisfies the requirements of 37 CFR §41.37(c)(1)(v). As such, it is believed that the Appeal Brief submitted on July 10, 2008 in respect of this application, when read to include the present Amended Summary of Claimed Subject Matter, is in full compliance with 37 CFR §41.37. Consideration of the aforementioned Appeal Brief by the Board of Patent Appeals and Interferences and reconsideration of the rejections and objections is requested. Allowance of claims 35-42, 44-50 and 52-82 at an early date is solicited.

Respectfully submitted,

Dated: November 3, 2008

Sanrø Zlobec
Reg. No. 52,535
Agent for the Applicant

SMART & BIGGAR
1000 De La Gauchetière Street West
Suite 3300
Montreal, Quebec H3B 4W5
CANADA

Customer Number: 28291

Telephone: (514) 954-1500
Facsimile: (514) 954-1396